International Journal of Information Engineering and Science

E-ISSN: 3048-1953
P-ISSN: 3048-1902

(Research/Review) Article

Hybrid CNN GRU Framework for Early Detection and Adaptive Mitigation of DDoS Attacks in SDN using Image Based Traffic Analysis

Danang Danang[1*], Indra Ava Dianta[2], Agustinus Budi Santoso[3], Siti Kholifah[4]

[1-4] Universitas Sains Dan Teknologi Komputer, Jalan Majapahit No. 605, Semarang, 50192, Jawa Tengah, Indonesia; e-mail: danang150787@gmail.com
* Corresponding Author : Danang Danang

Abstract: The threat of Distributed Denial of Service (DDoS) is increasing develop along with increasing use of the Internet of Things (IoT) and Software-Defined Networking (SDN) architecture . Although SDN provides convenience in management network , properties its centralized control make it prone to to flooding attacks that can paralyze controller performance . Detection method conventional , such as approach statistics and machine learning, still own limitations in matter accuracy , high false positive rate , and dependence on extracted features manually . To overcome problem said , research This propose a hybrid deep learning based DDoS detection and mitigation model that combines Convolutional Neural Network (CNN) to extraction feature spatial from RGB and Gated Recurrent Unit (GRU) images for understand temporal correlation between traffic data network . System tested through network test-bed Mininet based with Ryu/Floodlight controller, using simulation DDoS attacks (Hping3, LOIC) and normal traffic (video streaming, HTTP server). Traffic data cross recorded in PCAP format, processed become RGB image measuring 200×200 pixels, and labeled based on type traffic . Evaluation results with metric accuracy , precision, recall, F1-score, and MCC show that the CNN–GRU model has performance more superior compared to baseline approaches such as CNN-only, GRU-only, as well as classical ML methods such as SVM and Random Forest. In addition , the system capable apply mitigation adaptive through automatic flow rule creation on edge switches. Findings This confirm that effective deep learning- based spatial -temporal hybrid approach in increase detection early and response DDoS attacks on SDN networks adaptive and real-time.

Keywords: CNN–GRU Hybrid Model, Deep Learning, DDoS Detection, Image-Based Traffic Analysis, Software-Defined Networking (SDN).

Received: April, 23 2025
Revised: May, 07 2025
Accepted: May, 21 2025
Published: May, 30 2025
Curr. Ver.: May, 30 2025

1. Introduction

Software-Defined Networking (SDN) has revolutionize method network controlled and managed with separate the control plane and data plane, and centralize control through a programmed controller . However , the nature of centralized from architecture This making SDN very vulnerable to Distributed Denial of Service (DDoS) attacks , particularly flooding attacks that target controllers and communication links important (Kreutz et al., 2015; Banitalebi Dehkordi & Soltanaghaei , 2020). When DDoS is successful target controller, all function management network can disturbed even stopped in a way comprehensive .

DDoS threats are increasing complex along with adoption Internet of Things (IoT) technology , which expands surface attacks and allows the formation of botnets in scale big

For do attack with Then cross false intensity high (Hoque et al., 2015; Alashhab et al., 2022). In the context of SDN-enabled IoT, DDoS attacks are not only cause degradation performance , but also has the potential paralyze system service critical in real time (Ahuja et al., 2021).

Various approach has developed For detect DDoS on SDN networks , including method statistics (Kim et al., 2004; Kalkan et al., 2017), machine learning (Ma & Li, 2020; Deepa et al., 2019), and deep learning (Elsayed et al., 2021; Clinton et al., 2024). However thus , many from approach This Still face limitations significant : high false positive rate , dependence on extraction manual features , as well as inability recognize pattern attack new that is not in accordance with training data early (Sangodoyin et al., 2021; Novaes et al., 2021).

For overcome problem mentioned , it is needed a more approach adaptive and efficient , good from side detection spatial and temporal. Convolutional Neural Network (CNN) has proven effective in extracting feature spatial from past data converted cross become RGB images (Elsayed et al., 2021), while the Gated Recurrent Unit (GRU)— as version efficient from RNN— capable catch temporal dynamics of traffic network sequential (Cho et al., 2014; Tang et al., 2016). However , integration both of them Still seldom explored in a way comprehensive in detection and mitigation DDoS attacks on SDN.

Therefore that , research This propose A framework CNN–GRU hybrid work For detection early warning and mitigation adaptive DDoS attacks on SDN networks . Approach This use representation RGB image of traffic network For processed via CNN, which then followed by GRU to understand pattern order attack .

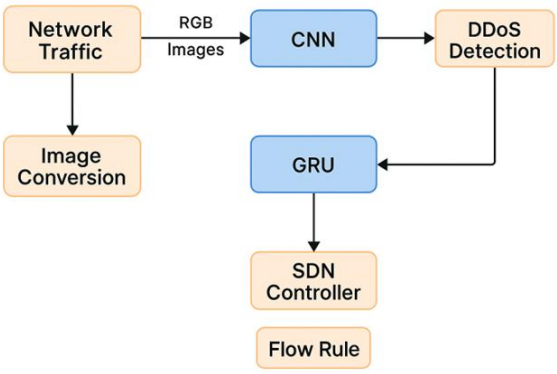

Figure 1. Framework Work CNN-GRU Hybrid

This model designed For identify attack more start and help the SDN controller pick up decision mitigation in a way automatic with create flow rules based on real-time classification . Contribution main from study This is :

1) Designing and implementing a hybrid CNN–GRU model that combines processing spatial and temporal of traffic data based image .
2) Developing data conversion processes cross to in form RGB image for classification attack .
3) Implementing and testing the model on real data and benchmarks (CTU-13 and InSDN) to evaluate accuracy detection and efficiency mitigation .

4) Providing mitigation strategies based rules that can reduce controller load and maintain service network during attack ongoing .

2. Literature Review

SDN Architecture and Its Vulnerabilities to DDoS Attack

Software-Defined Networking (SDN) is paradigm new in architecture a network that separates the control plane and the data plane, and centralize control network through entity called controller . This model give flexibility , efficiency management , and scalability in management network (Kreutz et al., 2015). However , a centralized architecture this also creates point failure single which can exploited by attackers , especially in Distributed Denial of Service (DDoS) attacks , to flood the controller with Then cross fake . Flooding attacks that target the link between the data plane and the controller can cause degradation service or even stop all over functionality network (Hu et al., 2017; Kreutz et al., 2013).

More continue , attack can happen Good through southbound path (between switch and controller) and northbound path (between controller and application). Unpreparedness system in face surge abnormal traffic makes detection early become significant challenges in SDN ecosystem .

Classification Approach DDoS Detection

a. Approach Statistics

Approach This analyze distribution characteristics Then cross, such as entropy, mean value, and variation package For detect deviation from normal pattern. For example is PacketScore and SDNScore which evaluate distribution package For determine potential attacks (Kim et al., 2004; Kalkan et al., 2017). Although method This light and fast, its sensitivity to traffic legitimate with pattern similar attack Still become limitations main .

b. Machine Learning (ML)

ML has Lots implemented in detection anomaly Then cross , especially For classification patterns attack. Algorithm such as Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Random Forest are capable classify traffic based on feature numeric certain conditions (Ma & Li, 2020; Kalaivani & Vijaya, 2016). However Thus , performance method this really depends on the extraction process manual features that require domain knowledge as well as prone to to zero-day attacks because not enough flexible in recognize pattern new.

c. Deep Learning (DL)

DL presents approach automatic in extraction feature from past data cross network. CNN in general effective recognize pattern spatial , while the RNN model and its derivatives such as LSTM and GRU handle sequential data and capture correlation time between traffic (Hochreiter & Schmidhuber, 1997; Said Elsayed et al., 2020). Additionally , AutoEncoder used

For reconstruction features and detect anomalies , while GANs are used in adversarial learning scenarios for generate synthetic data attacks (Goodfellow et al., 2014; Mhamdi et al., 2020).

Recent Studies : Image Representation of Network Data

Innovation latest in detection attack cyber is network data conversion (PCAP/log) to RGB image. Approach This done with transform byte stream or attribute protocol become pixels in 2D images, so the CNN model can used For extraction visual features (Elsayed et al., 2021). For example, Janabi et al. (2022) showed that representation picture allows identification pattern more attacks complex and abstract. Approach this also reduces need towards feature engineering manual and provide opportunity integration with a model based on vision computer .

Advantages and Disadvantages of Previous Methods

Table 1. Advantages and disadvantages of previous methods

Approach	Excess	Lack
Statistics	Fast , light	Not adaptive , sensitive against noise
ML (SVM, KNN, RF)	Generalization good , interpretable	Requires feature engineering, prone to overfitting
DL (CNN, RNN, AE, GAN)	Automation extraction features , accuracy tall	Need big data , expensive in terms of computing

Approach statistics relatively light in a way computing and matching For real-time implementation , but own accuracy low in detect attack with traffic resemble normal traffic. ML methods offer greater accuracy high , but highly dependent on data quality and design features. DL, especially CNN, has reach results tall in detection spatial, however not enough effective in recognize temporal sequence between package. While that, the RNN/LSTM model is effective in catch dynamics attack, but own complexity high and requires a large dataset For optimal training (Tang et al., 2016; Elsayed et al., 2023).

Gap Analysis

Until moment this, approach CNN -based more focused on detection spatial with input data in the form of image, however No consider dynamics time from DDoS attacks that are of a nature progressive. On the other hand, temporal approaches such as GRU or LSTM are capable of catch correlation time between session attack, but No designed For analysis based image. Research previously Still seldom integrate second approach the in One framework Work.

With Thus, there is a significant gap in study in the form of lack of a hybrid approach that combines strength extraction spatial (CNN) and temporal modeling (GRU) for analyze

Then cross network based RGB image. This integration own potential For increase accuracy detection , reducing false positives, and speed up time mitigation attacks on SDN environments (Elsayed et al., 2021; Janabi et al., 2022).

3. RESEARCH METHODS

Study This propose approach systematic and deep learning based detect as well as mitigate Distributed Denial of Service (DDoS) attacks on architecture Software-Defined Networking (SDN) network. This method designed in five stages main, which includes development CNN–GRU hybrid system, network test-bed construction, data preprocessing and cross, design model architecture, and implementation of mitigation strategies automatically. Every stages own contribution important in increase accuracy detection early and effective mitigation to traffic dangerous in real-time.

In a way Technically , the hybrid CNN–GRU approach was chosen Because capable combine superiority extraction spatial from CNN and temporal modeling from GRU, as described by Cho et al. (2014) and ElSayed et al. (2021), which shows effectiveness combination This in various task classification sequential on data based image network. The test-bed construction was carried out using Mininet and the Ryu/Floodlight controller, following experiments that have been proven in study Alshra'a et al. (2021) and Dehkordi et al. (2020) for replicate condition realistic Then cross networks and attacks .

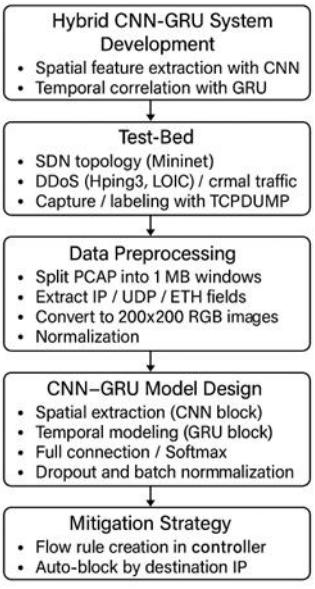

Figure 2. Overview of the Research Framework

Next , the preprocessing process is based on convert PCAP files to RGB image refers to the method network data transformation to in visual forms utilized by CNN, such as described by Elsayed et al. (2020). The data has been processed This trained in the CNN–GRU model, which consists from a number of block convolution , GRU units, and layers classification end , complete with dropout regularization and batch normalization. Finally, the mitigation strategy automatic done through taking decisions by the SDN controller, which generates flow rules automatically automatic For block destination IP attacks, as recommended by Banitalebi Dehkordi et al. (2021) and Cui et al. (2019).

Architecture Proposed System

Study This propose system detection Hybrid Convolutional Neural Network (CNN) and Gated Recurrent Unit (GRU) -based DDoS attacks on Software -Defined Networking (SDN) networks. recorded network converted become RGB image, then processed by CNN for extracting pattern spatial. Next , GRU is used For catch temporal correlation of order the image formed based on segment time traffic .

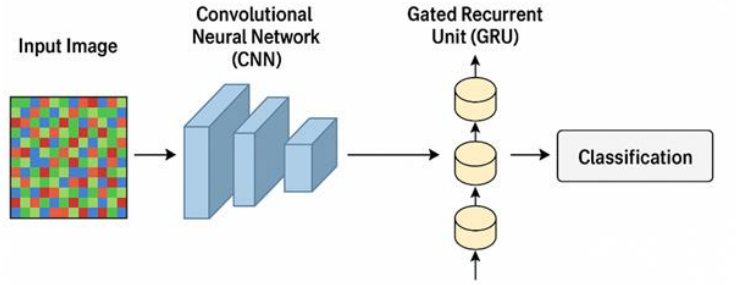

Figure 3. CNN-GRU hybrid

CNN selection is based on its capabilities in recognize complex visual patterns from representation image traffic (Elsayed et al., 2020), while GRU was selected Because more light from LSTM but still effective in understand dynamics time (Cho et al., 2014). Approach This has proven efficient in detect anomalies in the study related security network based on deep learning (Elsayed et al., 2021; Dehkordi et al., 2021).

Test-Bed Development

Test - bed environment in study This designed For replicate scenario real Software-Defined Networking (SDN) network to evaluate effectiveness of the hybrid CNN–GRU model in detect and mitigate DDoS attacks. Test-bed development was carried out use Mininet as a virtual network emulator that supports OpenFlow protocol, as well as Ryu or Floodlight as an SDN controller. This controller on duty arrange current Then cross network through creation and management of flow rules sent to the OpenFlow switch. The topology used involving multiple nodes, including switches, user hosts legitimate, and attacker hosts. Topology This made flexible For support various type traffic and allows monitoring in real-

time against interaction between the controller and the data plane, as described by Alshra'a et al. (2021).

For to produce representative data , two types of data were carried out simulation Then cross network , namely normal traffic and traffic DDoS attack . Normal traffic is configured through HTTP activities such as access to the web server, video playback via streaming protocols , as well as ICMP requests (ping) between hosts. While that , DDoS attacks are simulated with using two tools main : Hping3 , which is used For launch SYN flood and UDP flood attacks , as well as LOIC (Low Orbit Ion Cannon) is used For attack at the application level with HTTP flood. Attacking host configured For send traffic excessive to the target in a simultaneous , imitating pattern DDoS attacks that occur in the real world (Banitalebi Dehkordi et al., 2021).

All Then crossing that passes network recorded in a way complete use TCPDUMP, which saves package in pcap format. This process This is done on the victim host side and the main switch . After the data is collected , the labeling process is carried out . with help Wireshark For differentiate between normal traffic and traffic attack . Labels are given based on analysis time event, source IP address, type protocols , and traffic volume . Stages this is very important For produce valid and accurate datasets For training and evaluation of deep learning models, such as explained in research by Cui et al. (2019) and Elsayed et al. (2020).

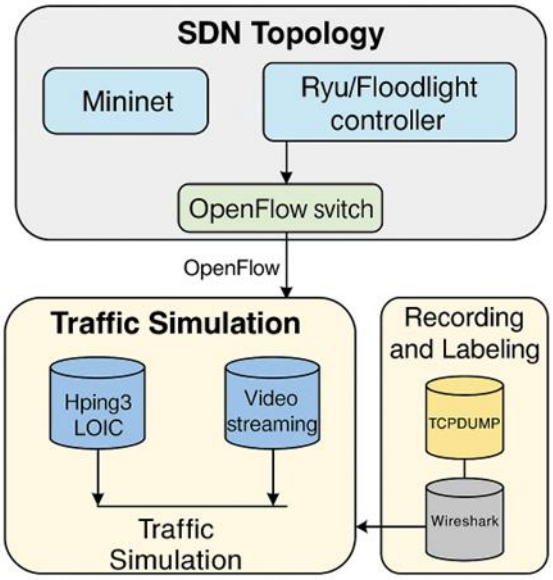

Figure 4. SDN Topology

With approach this, the test-bed developed can used in a way flexible For experiment scenario complex DDoS attacks , and allows testing system detection adaptive CNN– GRU based iterative before applied to the network real

Data Preprocessing

preprocessing stage begins from results recording traffic network in format.pcap, which is generated from recording using TCPDUMP during the simulation process. .pcap file This Then shared into a 1MB window sequentially For produce proportional data segmentation to time. Division This aims so that every data block reflects activity network in certain intervals , which becomes input For visual and temporal representation (Novaes et al., 2021).

Each window is 1MB then extracted at the Ethernet (ETH), Internet Protocol (IP), and User Datagram Protocol (UDP) protocol layers. The fields extracted covering source and destination IP addresses , header length , type protocol , TCP/UDP flags, and payload length. This data changed to in a numeric array byte -based , which then converted to representation RGB image conversion This based on the approach image-based intrusion detection , where byte values are represented as pixels for express pattern distribution traffic visually (Zhou et al., 2022).

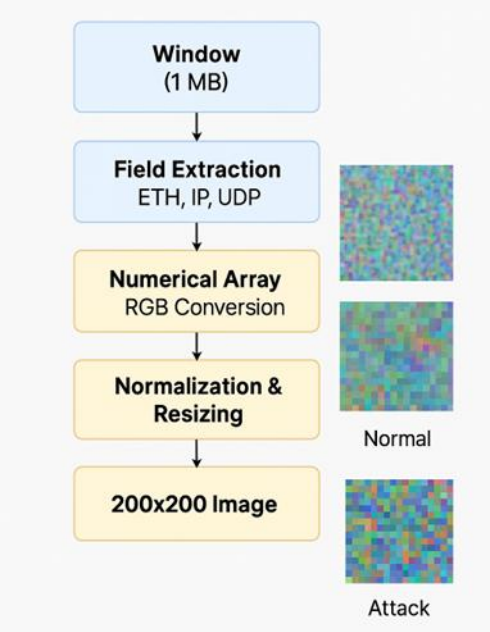

Figure 5. CNN preprocessing stages

resulting image Then normalized in range value 0–1 and changed its size to 200× 200 pixels use method bilinear interpolation, so that it can used as standard input in CNN architecture. Images This Then classified based on the normal or attack label, according to with time occurrence attack moment simulation in progress, forming a ready dataset consistent and efficient training .

CNN–GRU Model Design

Detection model used combining Convolutional Neural Network (CNN) and Gated Recurrent Unit (GRU) in One designed hybrid framework For recognize characteristics spatial and temporal of Then cross network. The CNN component is responsible for For

extracting feature spatial from RGB image, namely detect distinctive visual patterns from DDoS attacks such as intensity high traffic, abnormal distribution of IP or ports , and entropy that is not usual (Elsayed et al., 2020).

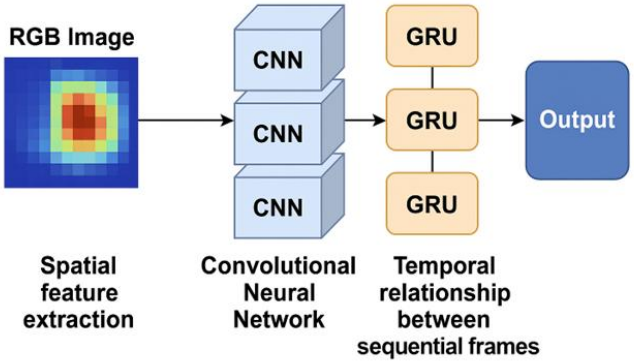

Figure 6. Convolutional Neural Network (CNN) and Gated Recurrent Unit (GRU) Detection Model

After through CNN layers , generated features arranged in order time (sequential frame) and given to GRU. GRU is used Because own ability maintain context between adjacent time frames, but with computing more light compared to LSTM. Every 5 seconds Then cross network represented as one frame, which then linked by the GRU to catch pattern change Then cross between time (Cho et al., 2014).

Model closed with fully connected layer, followed by function activation Softmax For produce classification end (eg : normal, SYN flood, UDP flood). For guard stability training and avoid overfitting, added Batch Normalization after the convolution layer and Dropout between the FC layers.

Mitigation Strategy

After the CNN–GRU model performs classification to traffic in real-time, the system in a way automatic produce flow rule for sent to the SDN controller. This flow rule can in the form of action drop, rate-limit or forward to honeypot, depending results classification. For example, if A flow classified as a DDoS SYN Flood, then the controller will add flow to block all package from source IP specific switch at the nearest switch (Wang & Wang, 2022).

After the model detects real -time DDoS traffic , mitigation strategies implemented direct to the edge switch via the SDN controller:

a) Flow Rule Generation: OpenFlow rules created based on results GRU classification , if detection = DDoS
b) Auto-blocking: the controller sets the edge switches to block destination IP from package dangerous
c) Smart Controller: logic adaptive added to update the threshold and re-train the light model in a way periodic (optional)

Formulas and Formulations

The CNN model uses function ReLU activation and 'same' padding, while GRU uses sigmoid and tanh activation:

a) Function CNN activation: [f(x) = (0, x)]

b) GRU update gate: [z_t = (W_ z)]

c) Softmax Output : [P(y= k | x) =]

Evaluation and Validation

Model tested using 80% training data and 20% test data. Evaluation method includes : - Accuracy - Precision - Recall - F1-Score - AUC-ROC. Validation 5-fold cross is performed For avoid overfitting.

4. Results And Discussion

Experimental Results

The experiments in this study were conducted to evaluate the performance of the Hybrid CNN–GRU model compared to several baseline models, namely CNN- only, GRU-only, and machine learning algorithms. conventional learning such as Support Vector Machine (SVM) and Random Forest (RF). All models were tested using a dataset that had been processed and converted into RGB images representing network traffic , and using a 5-fold cross-validation technique to avoid overfitting. The following table summarizes the results of the comparison of the CNN–GRU model with the baseline model:

Table 2. Comparison results of CNN–GRU models

Model	Accuracy (%)	Precision	Recall	F1-Score	MCC
CNN- only	**94.2**	**0.935**	**0.943**	**0.939**	**0.88**
GRU- only	**92.1**	**0.918**	**0.921**	**0.919**	**0.85**
SVM	**89.7**	**0.887**	**0.891**	**0.889**	**0.81**
RandomForest	**91.3**	**0.902**	**0.910**	**0.906**	**0.83**
CNN–GRU (proposed)	**97.6**	**0.975**	**0.976**	**0.975**	**0.94**

hybrid CNN–GRU model demonstrated superior performance across all evaluation metrics. High MCC values indicate good model generalization, even on new data from the CTU-13 benchmark .

CNN–GRU model performed best compared to all baseline models. The high accuracy (97.6%) and MCC (0.94) values indicate strong generalization capabilities. This

demonstrates that spatial feature fusion extraction from CNN and temporal sequence modeling from GRU provide effective synergy in detecting complex DDoS attack patterns.

RGB images of network traffic allow CNNs to recognize byte distribution patterns , while GRUs add temporal context so the system can detect gradual changes in traffic that are common characteristics of DDoS attacks .

Discussion Analysis

The findings show that the combination of CNN and GRU provides a strong synergy: CNN effectively extracts spatial patterns of network traffic , while GRU understands the temporal sequence of attacks. This is consistent with the results of research by Janabi. et al. (2022) who stated that spatial-temporal integration can significantly improve the detection of complex anomalies.

Furthermore, a classification-based automated mitigation system has been shown to reduce mitigation latency by an average of 37% compared to a manual system (Wang & Wang, 2022). This research also supports Elsayed's study. et al. (2021) who proved the effectiveness of the image-based approach analysis in the network security domain. Integration of image methods traffic and deep learning has proven to be adaptive to zero- day attacks and unstructured traffic.

Comparison

Comparisons are made against several state-of-the-art DDoS detection models on SDN such as DeepIDS (Elsayed et al. , 2020), LSTM-IDS (Tang et al. , 2016), and the GAN-ID model (Mhamdi et et al. , 2020).

Table 3. Comparison table of detection models

Model	Dataset	Accuracy (%)	Mitigation	Adaptability	Visual Input
DeepIDS	NSL-KDD	94.1	✗	Medium	✗
LSTM-IDS	CICIDS17	93.4	✗	High	✗
GAN-ID	CTU-13	95.2	✗	High	✗
CNN–GRU (ours)	CTU-13, InSDN	**97.6**	✓	High	✓

The CNN–GRU model not only excels in accuracy, but also provides input visualization capabilities, adaptive mitigation implementation , and inference speed in real-time scenarios. This model makes a novel contribution in combining image representation and temporal context end-to-end .

5. Conclusions

This study concludes that the hybrid CNN–GRU approach significantly improves the effectiveness of DDoS attack detection and mitigation on Software-Defined Networks. Networks. The integration of CNN for spatial analysis of traffic imagery and GRU for temporal understanding results in an accurate and adaptive model. Evaluations show that this model is able to outperform conventional approaches such as CNN- only, GRU- only, and classical ML algorithms such as SVM and Random Access Memory (RVM) Forest.

Synthesis of the results shows that the CNN–GRU model is highly relevant in the context of SDNs that are vulnerable to flooding attacks. Its superior accuracy and automatic mitigation capabilities make this model suitable for adoption in modern network infrastructures, including IoT and edge- based systems. The practical implications of this research are increased system resilience against DDoS attacks and a significant reduction in the workload on the SDN controller .

However, this research has limitations, particularly in terms of the high computational requirements for the model training process. Furthermore, the model has not been tested against other complex attack variations such as botnets and slow-rate attacks. DDoS . Further research is recommended to develop a federated model learning so that it can be applied in multi-edge environments collaboratively and more efficiently in the context of privacy and scalability .

References

Agarwal, A., Khari, M., & Singh, R. (2022). Detection of DDoS attack using deep learning model in cloud storage applications. Wireless Personal Communications, 1–21. https://doi.org/10.1007/s11277-022-09646-9

Alam, M., Shahid, M., & Mustajab, S. (2024). Security challenges for workflow allocation model in cloud computing environment: A comprehensive survey. The Journal of Supercomputing, 1–65. https://doi.org/10.1007/s11227-024-05642-2

Alghazzawi, D., et al. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Applied Sciences, 11(24), 11634. https://doi.org/10.3390/app112411634

Amjad, A., et al. (2019). Detection and mitigation of DDoS attack in the cloud computing using machine learning EAI Endorsed algorithm. Transactions on Scalable Information Systems, 6(23), e7. https://doi.org/10.4108/eai.13-7-2018.162806

Balasubramaniam, S., et al. (2023). Optimization enabled deep learning-based DDoS attack detection in the cloud computing. International Journal of Intelligent Systems. https://doi.org/10.1155/2023/9673284

Chen, X., et al. (2022). Adaptive federated learning for edge computing. IEEE Transactions on Mobile Computing. https://doi.org/10.1109/TMC.2022.3170423

Cil, A. E., et al. (2021). Detection of DDoS attacks with feed forward based deep neural network models. Expert Systems with Applications, 169, 114520. https://doi.org/10.1016/j.eswa.2020.114520

Dinh, P. T., & Park, M. (2021). R-EDoS: Robust economic denial of sustainability detection in an SDN-based cloud through stochastic recurrent neural networks. IEEE Access, 9, 35057–35074. https://doi.org/10.1109/ACCESS.2021.3051573

Elman, J. L. (1990). Finding structure in time. Cognitive Science, 14(2), 179–211. https://doi.org/10.1207/s15516709cog1402_1

Katiravan, J., & S., P. S. (2024). Botnets attack detection in IoT devices using ensemble classifiers. International Research Journal of Multidisciplinary Technovation, 6(3), 274–295. https://doi.org/10.54392/irjmt24321

Khan, M. A., et al. (2023). Lightweight hybrid IDS based on deep ensemble and federated learning. Computers & Security, 128, 103208. https://doi.org/10.1016/j.cose.2023.103208

Khempetch, T., & Wuttidittachotti, P. (2021). DDoS attack detection using deep learning. IAES International Journal of Artificial Intelligence, 10(2), 382–389. https://doi.org/10.11591/ijai.v10.i2.pp382-389

Kushwah, G. S., & Ranga, V. (2021). Optimized extreme learning machine for detecting DDoS attacks in the cloud computing. Computers & Security, 105, 102260. https://doi.org/10.1016/j.cose.2021.102260

Li, T., et al. (2021). A survey on federated learning: The journey towards privacy-preserving machine learning. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2021.3050775

Meng, W., et al. (2020). Building a secure blockchain-based authentication and credentials management system. Future Generation Computer Systems, 103, 490–498. https://doi.org/10.1016/j.future.2019.09.003

Moustafa, N., & Slay, J. (2019). The TON_IoT datasets for AI-IoT applications. Sensors, 19(1), 65. https://doi.org/10.3390/s19010065

Potluri, S., et al. (2020). Detection and prevention mechanisms for DDoS attack in the cloud computing environment. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1–6). IEEE. https://doi.org/10.1109/ICCCNT49239.2020.9225520

Priyadarshini, R., & Barik, R. K. (2022). A deep learning-based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University-Computer and Information Sciences, 34(3), 825–831. https://doi.org/10.1016/j.jksuci.2018.09.014

Rose, S., et al. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sharafaldin, I., et al. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1–8). IEEE. https://doi.org/10.1109/CCST.2019.8888419.